Management of Cyber Risks

Technology has played a transformative role in the provision of financial and payment services. In addition to improving the efficiency of processes, technology has opened up new and innovative channels for financial institutions to provide greater access and convenience to consumers. Technology has also enabled financial institutions to viably offer and manage a wider range of products that are competitive and responsive to different needs of consumers in ways that were not possible before. Business and retail customers have readily embraced these technological developments, as evidenced by the value of commerce transacted online which continues to rise.

These advancements however present new challenges for risk management by financial institutions. With increasing dependence on technology, financial institutions face new risks of malicious actions by criminals and other malefactors. These actions have the potential to disrupt the provision of services and also undermine the confidentiality and integrity of a financial institution's proprietary and customer data. Such incidents can thus damage the reputation of a financial institution and may undermine confidence in the financial system.

Global economic losses resulting from cybercrimes were estimated to be approximately USD375 billion annually[1]. Cyber attacks are commonly motivated by financial gain but can also be driven by an aim to cause disruption for social and political purposes. Following several high-profile cyber security incidents in the financial sector, the management of cyber risks has become an increasing global concern. A report[2] by the Committee on Payments and Market Infrastructure of the Bank for International Settlements emphasised the complex and rapidly evolving nature of cyber risks, and highlighted the increasing priority accorded to the effective management of these risks. The report also recommended a more integrated approach to cyber resilience, which will reduce recovery times in the event of a successful cyber attack, whilst enabling key functions of critical systems to continue to operate. In the European Union, the Joint Committee of the European Supervisory Authorities has similarly called for authorities and financial market participants to ensure that sufficient resources and attention are devoted to increasing the financial system's resilience against IT-related operational and cyber risks.

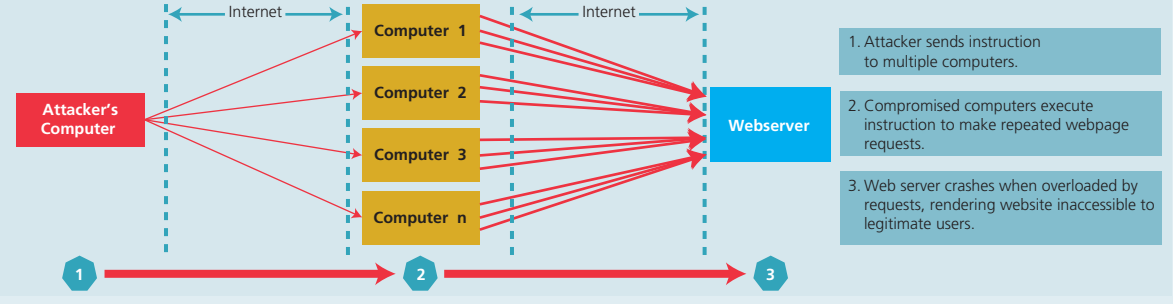
Forms of Cyber Threats

Cyber attacks against financial institutions are becoming more sophisticated and can take many forms. There are three common threats in the financial sector:

Distributed Denial of Service (DDoS) – In a DDoS attack, a targeted system is disrupted by directing a large flow of traffic to overwhelm it, thereby denying access by legitimate users. A network of compromised computers is directed to simultaneously make repeated requests (such as a particular web page) from the system (Diagram 1). Experts estimate that the number of DDoS attacks worldwide

Diagram 1

Distributed Denial of Service (DDoS) Attack on a Website



Source: Bank Negara Malaysia

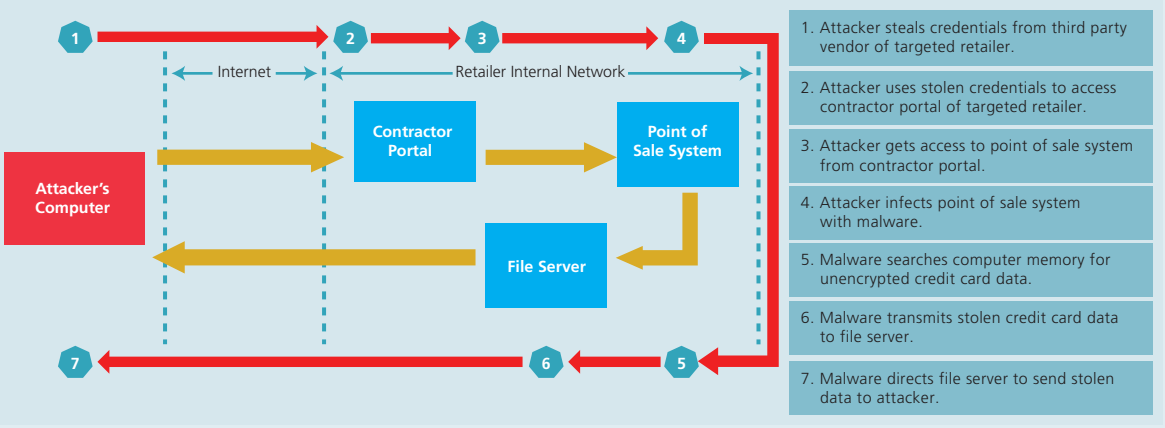
[1] Source: `Net losses: Estimating the global cost of cybercrime´, a report by the Center for Strategic and International Studies.
[2] Source: `Cyber resilience in financial market infrastructures´, November 2014.

have increased by 20% over the last two years, averaging almost 3,000 incidents per day, of which 43% were targeted at financial service providers[3]. DDoS attacks have been launched to disrupt customer access to the Internet banking portals of a number of global banks for hours or even days at a time, preventing customers from conducting online transactions. While DDoS attacks were experienced by some banks in Malaysia in 2014, this did not cause material service disruptions.

Malware – A malware attack involves the use of malicious software to control or disrupt the operations of a targeted system or device. Malware exists in many forms, such as viruses and worms, and can cause harm in different ways. One common form of malware in the context of financial services is the use of spyware installed on unsecured host machines to gather information about the user, which might include his Internet banking login credentials, credit card numbers, or other private or sensitive information. The information is then covertly transmitted back to the attacker for the purposes of committing fraud or other illegal activities (Diagram 2).

Diagram 2

Malware Attack on a Retailer



Source: Bank Negara Malaysia

Phishing – The most common form of fraud, phishing is the use of a fake website to induce an unsuspecting user to divulge sensitive information such as his Internet banking login and credit card details. The stolen information is then used to perform an unauthorised fund transfer or to commit other forms of fraud.

Criminals can combine different techniques to launch sophisticated attacks against systems. For example, malware can be used to take control of a large number of machines in order to carry out a DDoS attack. Such an attack would appear to come from a large number of unrelated sources and be more challenging to defend against. Similarly, by employing malware and phishing techniques, fraudsters can intercept Transaction Authorisation Codes (TAC) and perform fraudulent online banking transactions without the victim's knowledge.

Cyber attacks have also been used in combination with other conventional criminal activities. In 2014, malware was used to gain unauthorised access to 18 on-premise automated teller machines (ATMs) in Kuala Lumpur, Selangor, Johore and Malacca. In these incidents, criminals targeted several poorly guarded ATMs which were based on old models, gaining physical access to the internal components of the ATM and then installing malware into the operating system powering the ATM. The malware was specifically designed to compromise weaknesses in the outdated operating system of the ATMs. This subsequently allowed the criminals to direct the ATM to dispense cash without any authorisation or

[3] Source: Akamai, Arbor Networks.

verification. While the affected banks suffered losses of RM3.4 million, customers were not affected as the withdrawals were not debited from any customer accounts. The affected banks responded swiftly to upgrade the hardware and software of these and other similar ATMs. The banking industry has also since reviewed and implemented enhanced risk management practices and physical security measures to protect ATMs from further threats like these.

As increasingly sophisticated techniques are being employed to launch attacks, identifying and anticipating cyber threats and developing effective counter-measures remains a critical challenge. An organisation might also sometimes be unaware that it is a target of an attack. In what is termed as a `zero-day´ attack, an attacker exploits a vulnerability that is not known to the target, leaving the target no time or opportunity to patch the vulnerability. `Advanced persistent threats´, have also emerged in recent years with the capability to sustain a cyber attack, repeatedly over an extended period of time, while being able to adapt to efforts to resist it.

Industry and Regulatory Response to Cyber Threats

At the national level, initiatives to mitigate cyber security threats in Malaysia are pursued and coordinated with other government agencies as part of the National Cyber Security Framework. Under this national framework, the Bank and the financial institutions it regulates are deemed as Critical National Information Infrastructure (CNII), and thereby subject to heightened safeguards in recognition of their vital role to the country and economy. Important initiatives are pursued to continuously enhance the level of cyber preparedness of CNIIs. This includes annual cyber drills where simulations of cyber-attack scenarios are conducted to test the effectiveness of response programmes of each CNII and all CNIIs collectively against systemic attacks. Results of these exercises are then used to update and improve the response strategies and actions. Several financial institutions have been participating in these cyber drills since 2009 and have successfully completed the exercises by demonstrating the effectiveness of the respective incident response plans in managing the cyber-attack scenarios.

At the industry level, an Internet Banking Task Force (Task Force) established by the Bank and the banking industry supports a comprehensive regulatory response to cyber security threats. The Task Force provides a forum for financial institutions to share intelligence and discuss issues that concern Internet banking, including that on cyber security. Through this Task Force and other platforms, the Bank and the industry engages actively with other government agencies which include the Malaysian Communications and Multimedia Commission, CyberSecurity Malaysia and the Royal Malaysia Police. These engagements enable all stakeholders, including telecommunication companies and Internet service providers, to remain well-informed of latest developments in and emerging threats faced by the financial sector, while continuously promoting the adoption of industry best practices on Internet banking security. For example, the Task Force was instrumental in mitigating the threat of SMS-based scams which were prevalent several years ago. The Task Force shared technical details and information regarding the modus operandi of the scam which enabled weaknesses in the existing processes to be identified and addressed, such as by requiring certain Internet banking customers to register in person at a branch. These measures resulted in a significant decrease in the incidence of SMS-based scams. In its capacity as the competent authority for receiving and analysing information on suspicious transactions, the Bank also disseminates financial intelligence related to persons suspected to facilitate the transaction and mule account holders[4] to support investigations by law enforcement agencies and to reinforce joint efforts in combating cyber crime.

At an institutional level, financial institutions have continued to evolve a wide range of defensive tactics and IT security practices to deter and defend against emerging cyber threats. These include:

- the segmentation of network zones to control user access and limit the propagation of any threats that manage to penetrate the network;
- implementing redundant controls in multiple layers of the network infrastructure (defense-in-depth) so that the failure of one control measure is mitigated by controls in other layers;

[4] People who allow their bank accounts to be used by criminals to hold or transfer money which is acquired illegally.

- deploying appropriate network security tools such as intrusion prevention system (IPS) and the use of multiple firewalls, including the web application firewall (WAF) as an enhanced DDoS mitigation strategy;
- conducting regular and rigorous security assessments on IT infrastructure, including stringent penetration tests. The scope of penetration tests have also been enlarged to include mobile-based applications;
- ensuring constant security monitoring and surveillance to enable the early detection of intrusions; and
- establishing computer emergency response teams to improve response times to cyber incidents.

The effectiveness and consistency of these practices are also regularly reviewed by the auditors of the financial institutions, and any identified weaknesses are promptly highlighted for rectification. Nevertheless, the proper management of cyber security risks is ultimately a board-level responsibility. The Bank expects boards of financial institutions to ensure that sufficient priority and resources are allocated to the oversight and management of these risks. Some boards have already made progress in this area as evidenced by more robust discussions on risk management strategies and a deeper understanding of the more technical aspects of cyber security.

On its part, the Bank had issued various guidelines to specify minimum standards to be observed by financial institutions in the provision of electronic banking services and the management of IT systems and networks. From time to time, these are supplemented by additional guidance published by the Bank to confront specific threats, such as detailed requirements to strengthen security controls on public Internet banking kiosks and to enhance preparedness against DDoS attacks. The Bank is currently in the process of reviewing and updating existing regulatory standards and guidance to further strengthen IT security standards across the financial sector and improve the industry's defense and response to evolving cyber threats. The key objectives of the new standards to be issued in 2015 are to:

- strengthen governance over cyber security in financial institutions;
- ensure that adequate strategic focus and resources are directed by financial institutions at the management of cyber security risks;
- provide practical guidance that reflects the changing technological landscape and business models, and is sufficiently flexible to adapt to new threats;
- increase the rigour of financial institutions' assessment of cyber threats and the quality of information used to inform such assessments;
- further improve recovery plans and contingency or business continuity arrangements; and
- promote more robust due diligence of critical third party service providers.

To ensure that consumers are also able to protect themselves against these cyber threats, efforts have also been directed by the Bank together with the industry, to promote awareness on safe online practices. Aside from continuous consumer education programmes, financial institutions have also stepped-up efforts to provide online banking security tips on their websites.

As existing IT security methods and tools are constantly facing newer threats, the financial sector must remain vigilant against potential vulnerabilities within its critical systems, and continues to update its defenses and strengthen its strategies to mitigate and manage emerging cyber risks. This will include improving intelligence gathering capabilities as well as adopting a more integrated and coordinated approach in dealing with cyber threats.